

Sharing Without Disclosing: Analysis on the Protocols

Azra siddiqui, Shumail Ahmad Siddiqui

¹School Of Electrical And Information Technology, WITS University

²Tata Consultancy Services

siddazra@gmail.com, siddiqui.shumail@gmail.com

Abstract—In many of today's business and government identity programs, smart cards based application are becoming more prevalent. Strong cryptographic algorithms are needed to protect the data stored on the card. Smart card with embedded microcontroller has outstanding property to securely store the data and to perform the on-card functions like encryption and digital signature. In many applications it is important to share information without exposing private details. In this paper we will find ways to protect data while also allowing it to be compared with other party.

Keywords: Cryptography, erasures, smart cards, secure computation, sharing data.

I. Introduction

Megabytes of information can be stored in smart cards even the important secrets such as DES keys and RSA private keys. Two things that it requires is data authentication and confidentiality. Having several applications on one smart card there are several concerns against attackers such as timing attack and differential power analysis. Serpent and Two fish algorithm applied on smart card never allow data to slip from power analysis[1]. Thus the attackers now won't be able to measure the patterns of signals to noise ratio and so cannot measure the power consumption of the card. Out of two differential power analysis and timing attacks on smart cards. The DPA problem is recommended to be solved using the above two mentioned algorithms.

II. Crypto Flaws

Randomness in random number generator for cryptographic keys is a crucial ingredient in ensuring opponents can't break the crypto keys underpinning the smart cards. The team of researchers examined that out of 2 million 1024 bit RSA keys 184 keys were generated so poorly that they could be broken in a matter of hours using some mathematical methods and standard computer system to find large prime numbers at their core[2]. The above was the flaws that occurred in Taiwan's secure digital ID system that allow attackers to impersonate some citizens who rely on it to pay taxes, and file immigration papers, etc.

Mifare DESfire MF3ICD40, a widely used RFID smart card has also gone through the cryptographic flaws on the smart card. The attacker used a templated "side-channel" attack on the card. It requires the attacker to have an RFID reader, and a radio probe and a card itself. Using DPA, data is collected from radio frequency energy that leaks out from the side channels of

the card. Through this process, Oswald and Paar were able to retrieve the entire 112-bit secret key from the MF3ICD40, which uses Triple DES encryption [2].

III. Commitment Scheme with Non - Interactive Opening Algorithm

The Universal Composability (UC) framework is a security paradigm which guarantees that a protocol proven secure in this framework remains secure with other concurrently running protocols and even enables one to split the design of complex protocol to simpler sub protocols. One of the fundamental primitive in cryptographic protocol theory is commitment scheme. In this scheme one of the party makes commitment that out of some finite set he will choose a value m and can no longer will change his mind. Moreover he does not have to reveal his choice. This is usually called **binding property**. When the receiver gets the sealed value of m from committer he cannot tell what is inside until committer decides to give him the keys. It is required that receiver cannot learn anything about m . This usually is called **hiding property**. The reason we are interested in making such commitment scheme is that its functionality enables the accomplishment of secure protocols that accomplish surprisingly complicated and impossible tasks.

IV. Two Party Computations

The parties P_1 and P_2 with private inputs x_1 and x_2 wish to compute a joint function f of their inputs while preserving secure properties like privacy (nothing but the output is revealed), correctness (the correct output is obtained) and independence of inputs (no party can choose its input as a function of other party's input). Let's understand it by taking the example of sharing data among parties in an election. By **privacy** we mean that individual votes are not revealed, by **correctness** we mean that candidate with majority votes win and by **independence of inputs** we mean that other party cannot vote as the function of the outcome. Of course the security in two party computation must be guaranteed as the adversary may be **semi honest** or may be **malicious**. Semi honest adversary follows the protocol exactly but attempts to get more information by analysing the received message whereas malicious adversary may arbitrarily deviate from the specified protocol so fair results may not be achieved.

V. Lindell's And Yao's Protocol

Since the 1980's the feasibility of secure computation has been deeply studied. Yao's protocol is for secure two party computation has a constant number of rounds and some symmetric encryptions per gate. It was believed that protocol

based on circuit for computing the function can never be practical, but in 2004 the first secure computation protocol for semi honest adversary was carried out. Millionaires problem on 32 bit integers took 1.25 seconds in LAN and 4.01 seconds in WAN. The drawback was that these protocols need exponentiation per gate and was efficient only for small circuits. In recent years based on Yao's garbled circuit construction, an approach was used to design more efficient protocol. In Yao's garbled circuit computation, garbling means encryption of the circuit with following conditions:

1. With each input wire two secret keys are associated (one for 0 bit and other for 1 bit).
2. Given the keys associated with bits $a_1 a_2 a_3 \dots a_n$ belongs to set $\{0,1\}$, it is possible to compute the associated output $f(a_1, a_2, a_3, \dots, a_n)$ and not possible to learn anything beyond $f(a_1, a_2, a_3, \dots, a_n)$.
- 3.

A. Working Of Yao's Protocol

Party P1 constructs a garbled circuit computing the function f and sends it to party P2. Party P1 also sends the keys associated with its input a to party P2. Both P1 and P2 run 1-out-of-2 oblivious transfer (OT) for every bit of P2's input. In the i th OT, P2 inputs b_i and P1 inputs the pair of keys k_i^0, k_i^1 associated with this input wire. P2 receives k_i power b_i . Given one key for every input wire, P2 computes the garbled circuit, obtains the output $f(a,b)$, and sends it to P1.

B. Working of Lindell's Protocol

The Lindell's protocol was based on two party commitment schemes in presence of adaptive adversaries with erasures. The term "Adaptive Adversary" refers to an adversary who will shift his focus in response to newly deployed defensive measures. His model with erasures means that the honest party should need to erase data so that it is not available to adversary. For measuring security Lindell defined two models – ideal and real. The ideal model has two parties P1 and P2, adaptive semi honest adversary \tilde{A} and a trusted third party. Each party has security parameters in unary form and designated inputs. Input a for P1, input b for P2 and input c for \tilde{A} . Adversary \tilde{A} can get the appropriate party's input by issuing any corrupt command. Party P_i sends its input to trusted party which then computes $(x_1, x_2) = f(a, b)$ and gives each P_i the value of x_i . The adversary receives the output from the corrupted party and proceeds to another corruption phase.

In real model everything is same except the trusted third party. The parties P1, P2, and \tilde{A} run the protocol which includes the erase command also. The adversary may corrupt the honest parties and can receive all the information and history of the party except the data that has explicitly deleted. At the end all the parties output the correct output except the adversary \tilde{A} which outputs an arbitrary function of its view in the execution. Having compared the Ideal and real model we can say that they simulate each other. For semi honest adversaries Lindell pointed out that OT that is secure for static adversary can obtain addition adaptive security with erasures. This can be done by exchanging the actual bit with the random values obtained from the secure oblivious transfer with random inputs.

For malicious adversary he observed and proved that any protocol that is adaptively secure in a model with ideally secure communication channels can be converted into an adaptively secure protocol with authenticated communication channels, assuming erasures.[5]

V. Analysis And Comparison Of Lindell's And Yao's Protocol

Yao's protocol is designed for both semi honest and malicious adversaries. From security point of view he has optimised his circuit with following add ons

Optimization in circuit for semi honest adversaries:

1. double –encryption optimization
2. Free XOR gates.
3. Garbled row reduction
4. Circuit optimization using less XOR and AND gates.
5. Oblivious transfer extensions.
6. Pipelined Execution.

Optimization in circuit for malicious adversaries:

1. The Yao's garbled circuit for malicious adversary can compute different functions of the elevator's input thereby revealing the secret. Cut-and-choose paradigm can be used for correcting the circuit.
2. Selective bit attack is another problem which can be solved by randomizing the inputs or incorporating the input keys for P1 into the checks.

To enforce input consistency it is possible to optimize it but it means massive parallelism is needed. So the security cost is going to be very high. At this stage we may say that Yao's can't go further and there is still more to do.

Lindell has presented two efficient commitment schemes, one proven against static adversaries and other against adaptive corruptions. The security of both the schemes relies on Decisional Diffie Hellman assumption [3]. He stressed on the point that encryption scheme on Yao's garbled circuit must be secure for multiple messages. The problem of Yao's protocol is that how a receiver can know which value is intended decrypted. So in his protocol he imposed the special encryption under one key to never be a valid encryption on another key. Thus the receiver will take the single decrypted value as the key for the gate -output wire [4]. Lindell also proposed that for every bit of P2's input the parties run an OT protocol. With his protocol it is possible to securely compute the OT functionality assuming the existence of enhanced trapdoor permutations. Moreover, secure encryption schemes can be constructed from one way function.

VI. Conclusion

No single security mechanism provide complete security and, indeed complete security doesnot exist. The objective here in this paper is to analyse and implement the appropriate security measures to address the expected threats and risk by the adversary. though smart card technology is a critical element in

the chain of trust in secure system design but using Lindells and yao's protocol on it we secured it at number of levels. Lindell notes that high end smart cards have strong protection and can be designed to self destruct if the chip is compromised. Till no other privacy concerns are rising this protocol at least is currently giving the organization what they are needing. I firmly believe that we will start seeing secure computation in use in the near future

ACKNOWLEDGMENT

This research paper is made possible through the support and encouragement from our parents, family and friends. I sincerely thanks to my professors who have taught me cryptography and algorithms.

REFERENCES

- i. [1] James Nachvatal, Elaine Barker, Donna Dodson, Morris Dworkin, James Foti, Edward Roback. "Status Report on the First Round of the Development of the Advanced Encryption Standard". Computer Security Division, National Institute of Standards and Technology. <http://csrc.nist.gov/CryptoToolkit/aes/round1/r2report.htm>
- ii. [2] <http://arstechnica.com/security>
- iii. [3] Yehuda Lindell. Highly efficient universally composable commitments based on the DDH assumption. In Kenneth G. Paterson, editor, advances in cryptology – EUROCRYPT 2011, volume 6632 of lecture notes in computer science, pages 415-432.
- iv. [4] <http://eprint.iacr.org/2004>
- v. [5] D. Beaver and S. Haber. Cryptographic Protocols Provably Secure Against Dynamic Adversaries. In EUROCRYPT'92, Springer-verlag (LNCS 658).